1954

On the existence of simple difference sets for n less than 2500

Maynard Branson Stevenson
The University of Montana

ON THE EXISTENCE OF SIMPLE DIFFERENCE SETS FOR n LESS THAN 2500

by

MAYNARD B. STEVENSON

B.A. Montana State University, 1953

Presented in partial fulfillment of the
requirements for the degree of
Master of Arts

MONTANA STATE UNIVERSITY

1954

Approved by:

T. G. Ostrom
Chairman, Board of Examiners

Gordon B. Castle
Dean, Graduate School

Aug 13 1954
Date

ACKNOWLEDGEMENTS

The author is especially indebted to Professor T. G. Ostrom, who suggested the topic, for his guidance and numerous helpful suggestions in composing the paper; and to Professor J. Hashisaki for his assistance with the computations.

M.B.S.

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

A finite set of integers $\{a_i\}_{i=0}^{n}$, such that the set of differences $(a_i - a_j)$, where $i \neq j$, contains each non-zero residue (mod N) exactly once, is called a difference set (mod N). Obviously

$$N = \frac{(n+1)!}{(n-1)!} + 1 = n^2 + n + 1$$

and throughout this paper we will use N to denote $n^2 + n + 1$.

James Singer [1] has shown that there exists a difference set (mod N) whenever n is a positive integral power of a prime, and it has been conjectured that in no other case is there a difference set.

It is the purpose of this paper to show, using various theorems based on additive number theory, that the conjecture is true for n less than 2500. T. A. Evans and H. B. Mann [2] have shown that the conjecture is true for n less than 1600, and we shall have occasion to use many of their results as well as some theorems of Marshall Hall, Jr. [3] and T. G. Ostrom [4].

A knowledge of elementary number theory will be assumed on the part of the reader, but for clarity, a few of the basic definitions are listed below.

1) The set of consecutive integers 0, 1, 2, . . . M - 1 is called the least positive residue system (mod M).

2) If r and s are any two integers, we say r is congruent to s (mod M) and write $r \equiv s \pmod{M}$ in case $r - s = KM$ where K is an integer.

3) A complete residue system (mod M) is any set $\{a_i\}_{i=1}^{M}$ of M integers, no two of which are congruent (mod M).

4) r is called a quadratic residue (mod M) in case r is an integer, and if there exists an integer a such that: $a^2 \equiv r \pmod{M}$. (An analogous definition applies to congruences of higher order).

5) Let r and M be relatively prime integers. Then we say that r is of order K (mod M), (or that r belongs to the exponent K (mod M)), if $r^K \equiv 1 \pmod{M}$, where K is a positive integer not equal to zero, and $r^Q \equiv 1 \pmod{M}$ implies K divides Q. (Note: r and M must be relatively prime in order that the congruence $r^K \equiv 1 \pmod{M}$ have a solution).

6) For any positive integer M, $\Phi(M)$ denotes the number of positive integers relatively prime to M.

Definition (1): A finite projective plane is an arbitrary set of points $P_1, P_2, \ldots P_N$ such that there are $n^2 + n + 1$ subsets l_i called lines with the following properties:

1) If l_i and l_j are any two distinct lines, then there exists one and only one point P_k such that $P_k \in l_i$ and $P_k \in l_j$.

2) If P_i and P_j are any two distinct points, then there exists one and only one line l_k such that $P_i \in l_k$ and $P_j \in l_k$.

It is apparent that the number of points must be of the form $n^2 + n + 1$, the number of distinct lines in the plane is $n^2 + n + 1$, and the number of distinct points in a line is $n + 1$.

Definition (2): A mapping ψ in a finite projective geometry is called a collineation if ψ maps points into points and lines into lines. We say ψ has order e if ψ^e is the identity mapping, and if e is the smallest integer such that this is true.

Definition (3): A plane π is called cyclic with respect to a collineation ψ or a "cyclic projective plane" if the cyclic group $G(\psi)$ generated by ψ is transitive on the points of π. That is, given any two points P_i and P_j in π, there exists an element ψ^k in $G(\psi)$ such that ψ^k maps P_i into P_j. Choosing any point of π as P_o, the collineation ψ applied N times induces a cycle on the points of π.

CHAPTER II

SOME BASIC THEOREMS

In this chapter, the theorems necessary for showing that no difference set exists for a composite n = 2500 are presented, along with related notions and definitions. To facilitate reference, the theorems of the authors mentioned in chapter one will be numbered as in the publications in which they appeared. Where an author has theorems in more than one publication, the reference number will also be given.

The following theorem shows that the existence of a finite cyclic projective plane with N points implies the existence of a difference set (mod N), and conversely.

Theorem 1: (Hall's Theorem 2.1) Let the points on a line m_o of the cyclic projective plane π be given by

(2.3) $\quad m_o : a_o, a_1, \ldots, a_n \pmod N$.

Then if $d \not\equiv 0 \pmod N$ the congruence

(2.4) $\quad x - y \equiv d \pmod N$

has one and only one solution $x = a_i$, $y = a_j$ with a_i, a_j belonging to the set $a_o, a_i, \ldots, a_n$. Conversely a set $a_o, a_i, \ldots, a_n \pmod N$, $n \geq 2$, such that (2.4) with $d \not\equiv 0 \pmod N$ has one and only one solution $x = a_i$, $y = a_j$ from the

set determines a plane π whose points are the integers (mod N) and whose lines are given by $m_r: a_o + r, \ldots, a_n + r$ (mod N) (r reduced (mod N)) and the mapping $i \rightleftarrows \psi^d(i) = i + d$, (i reduced (mod N)) is a collineation of the plane π.

Proof: Given the cyclic projective plane π and the line m_o as given by (2.3). If $d \not\equiv 0$ (mod N) the line $m_d = \psi^d(m_o)$ is either identical with m_o or has exactly one point in common with m_o. A point in common to m_o and m_d may be written $p = a_i \in m_o$ and $p = a_j + d \in m_d$. Hence $a_i - a_j \equiv d$ (mod N) and $x - y \equiv d$ (mod N) has either 1 solution if m_o and m_d are distinct lines or n + 1 solutions if m_o and m_d are the same line with $x = a_i$, $y = a_j$. Since $N = n^2 + n + 1$, $a_i - a_j$, where $a_i \neq a_j$, has only $n^2 + n$ possible values and as each value $d = 1, 2, \ldots, N - 1$ is taken on it follows that each value is taken on exactly once. This proves the first part of the theorem for finite cyclic projective planes.

Conversely suppose a difference set $a_o, a_1, \ldots, a_n$ (mod N) given. Let every integer (mod N) be called a point and let lines m_r be defined to contain the points $a_o + r, \ldots, a_n + r$. If u and v are any two different points, let a_i and a_j be determined by $a_i - a_j \equiv u - v \equiv d$ (mod N). Then $u - a_i \equiv v - a_j \equiv e$ (mod N) and m_e contains $a_i + e \equiv u$ and $a_j + e \equiv v$, hence there is a line containing these two points. If there were more than one line containing two distinct points u and v a reversal of these congruences would show that $x - y \equiv d$ (mod N) would have more than one

solution $x = a_i$, $y = a_j$ from the difference set. Hence there is one and only one line through any two different points. Any two distinct lines m_r and m_s will have a point $a_i + r \equiv a_i + s$ in common where $x = a_i$, $y = a_j$ is the unique solution from the difference set of $x - y \equiv s - r \pmod N$. Hence there is one and only one point in common to two distinct lines. The condition $n \geq 2$ assures us that every line contains at least three points. Also the mapping $i \rightleftarrows \psi(i) = i + 1$ maps $m_r \rightleftarrows (m_r) = m_{r+1}$ and is a collineation of the plane.

Theorem 2: Given any difference set $\{a_i\}_{i=0}^{n} \pmod N$, the set $\{a_i + s\}_{i=0}^{n}$, where s is any integer, is a difference set (mod N), for $(a_i - a_j) = ((a_i + s) - (a_j + s))$.

Definition 4: An integer q is called a multiplier of a difference set $\{a_i\}_{i=0}^{n} \pmod N$ if and only if the set $\{qa_i\}_{i=0}^{n} \pmod N$ is the same as the set $\{a_i + s\}_{i=0}^{n} \pmod N$ in some order for some integer s.

Theorem 3: If $a \equiv b \pmod N$, then $X^a \equiv X^b \pmod{(X^N - 1)}$.

Proof: (I) (Given:

$$(1)\quad a - b = CN$$

where C is an integer, must show

$$(2)\quad X^a - X^b = K(X^N - 1)$$

where K is a polynomial in X.

$$X^a - X^b = X^b(X^{a-b} - 1).$$

By (1), $a - b = CN$, hence

$$X^b(X^{a-b} - 1) = X^b(X^{CN} - 1)$$

and now $(X^N - 1)$ divides $(X^{CN} - 1)$, so that (1) implies (2).

(II) (Given

$$(2)\quad X^a - X^b = K(X^N - 1)$$

must show

$$a - b + CN$$

where C is an integer).

$X^a - X^b = K(X^N - 1)$

$X^b(X^{a-b} - 1) = K(X^N - 1)$ and

$(X^N - 1)$ must divide X^b or $(X^{a-b} - 1)$. But $(X^N - 1)$ cannot divide X^b, hence must divide $(X^{a-b} - 1)$, but this implies $(a - b) = CN$, or $a \equiv b \pmod N$ so that now (2) implies (1).

Theorem 4: (Hall's theorem 4.1.) Let $\{a_i\}_{i=0}^{n}$ be a difference set modulo N, and write $\theta(X) = \sum_{i=0}^{n} X^{a_i}$. Then

$$\theta(X)\,\theta(X^{-1}) \equiv n + 1 + X + \ldots + X^{N-1} \pmod{X^N - 1}$$

Proof: $\theta(X)\theta(X^{-1}) \equiv \sum_{t=(a_i - a_j)} X^t \pmod{X^N - 1}$.

Since $a_0, \ldots, a_n$ is a difference set (mod N), the set of differences $(a_i - a_j) \pmod N$ is a complete residue system (mod N), plus n additional zeros, each non-zero residue (mod N) appearing exactly once. Hence, in view of theorem 3, theorem 4 follows at once...

Corollary 4.1: (Hall's Corollary 4.1) If σ is a root of $\frac{(X^N - 1)}{(X - 1)}$ then $\theta(\sigma)\,\theta(\sigma^{-1}) = n$.

Proof: Corollary 4.1 is obvious since

$$\theta(X)\theta(X^{-1}) = \frac{(X^N - 1)}{(X - 1)} + n.$$

Theorem 5: (Hall's Theorem 4.5) If p is a prime divisor

of n, then p is a multiplier of any difference set (mod N).

Proof: Let $\theta(X)$ be defined as in theorem 4, and applying theorem 3, we have:

4.8.1 $$\theta(X)\theta(X^{-1}) \equiv n + 1 + X + X^2 + \ldots + X^{N-1} \pmod{X^N - 1}$$

and since (N,p) = 1 we have:

4.8.2 $$\theta(X^p)\theta(X^{-p}) \equiv \sum_{t=(a_i-a_j)} X^{pt} \equiv \sum_{t=(a_i-a_j)} X^t \equiv n + 1 + X + X^2 + \ldots + X^{N-1} \pmod{X^N - 1}$$

Now alter the modulus of 4.8.1 to the double modulus $\left(p, \frac{(X^N - 1)}{(X - 1)}\right)$, and multiply 4.8.1 by $\theta(X)^{p-1}$ to obtain

4.9.1

$$\theta(X)^{p-1}\theta(X)\theta(X^{-1}) = \theta(X)^p\theta(X^{-1}) \equiv \theta(X)^{p-1}(n+1+X+\ldots+X^{N-1}) \equiv$$

$$\equiv \theta(X)^{p-1}\left(n + \frac{(X^N - 1)}{(X - 1)}\right) \equiv 0 \quad \operatorname{modd}\left(p, \frac{(X^N - 1)}{(X - 1)}\right)$$

Now by a well known theory of congruences, we can write:

4.9.2 $$\theta(X)^p\theta(X^{-1}) \equiv \theta(X^p)\theta(X^{-1}) \quad \operatorname{modd}\left(p, \frac{(X^N - 1)}{(X - 1)}\right)$$

hence

$$\theta(X^p)\theta(X^{-1}) \equiv 0 \quad \operatorname{modd}\left(p, \frac{(X^N - 1)}{(X - 1)}\right)$$

Now write the general congruence:

4.10 $$\theta(X^p)\theta(X^{-1}) \equiv e_0 + e_1X + \ldots + e_{N-1}X^{N-1} \pmod{X^N - 1}$$

which must hold for a certain set of e's as we have an e_i times every residue of the above modulus.

Now from 4.9.2 we know that:

4.10.1 $$\theta(X^p)\theta(X^{-1}) \text{ (reduced mod p)} \equiv 0 \pmod{1+X+\ldots+X^{N-1}}$$

4.10.2 $\Theta(X^p)\Theta(X^{-1})$ (reduced mod p) $= K_1(1 + X + \ldots + X^{N-1})$

Also, from 4.10 we know that:

4.10.3 $\Theta(X^p)\Theta(X^{-1}) - (e_0 + e_1X + \ldots + e_{N-1}X^{N-1}) = K_2(X^N - 1)$

hence

4.10.4 $\Theta(X^p)\Theta(X^{-1}) = (e_0 + e_1X + \ldots + e_{N-1}) + K_2(X^N - 1) =$

$= (e_0 + e_1X + \ldots + e_{N-1}X^{N-1}) + K_2(X-1)(1+X+X^2+\ldots+X^{N-1})$

and hence by 4.10.1 we can write:

4.10.5

$K_2(X-1)(1+X+X^2+\ldots+X^{N-1}) + (e_0+e_1X+e_2X^2+\ldots+e_{N-1}X^{N-1})$

(reduced mod p) $\equiv 0 \pmod{1 + X + X^2+\ldots+X^{N-1}}$.

But this implies:

4.11 $e_0 \equiv e_1 \equiv e_2 \equiv \ldots \equiv e_{N-1} \pmod p$

Hence we have in view of 4.10.5:

4.11.1 $$e_i = d + K_ip$$

where d is a least positive residue (mod p). Now the left hand side of 4.10 is a product of two polynomials with n + 1 terms each, each term having 1 as its coefficient. Since a reduction (mod $X^N - 1$) merely reduces the exponents of the x's without altering the coefficients, we have:

4.12 $$\sum_{i=0}^{N-1} e_i = n^2 + 2n + 1.$$

Also, we have:

4.12.1 $d + K_ip > 0$ (since $p > d$) and

4.12.2 $$\sum_{i=0}^{N-1} e_i = \sum_{i=0}^{N-1}(d + K_ip) \equiv Nd \pmod p$$

But we have $N = n^2 + n + 1$, and p divides n hence:

4.12.3 $$\sum_{i=0}^{N-1} e_i = n^2 + 2n + 1 \equiv (n^2 + n + 1)d \equiv 1 \pmod{p},$$

so $d \equiv 1 \pmod{p}$, but $d < p$ so $d = 1$, so by 4.11.1

4.13 $$e_i \equiv 1 \pmod{p}, \quad i = 1,2,\ldots N-1$$

and by 4.12.1 we conclude that $e_i > 0$.

Since the e_i's are non-negative integers, we can use the distributive law to write 4.10 as:

4.14 $$\Theta(X^p)\Theta(X^{-1}) \equiv 1 + X + \ldots + X^{N-1} + PR(X), \pmod{(X^N - 1)}$$

where if $n = pm$, $R(X)$ is the sum of one or more positive terms whose coefficients total m. Using an entirely analogous argument, and multiplying 4.8.1 by $\Theta(X^{-1})^{p-1}$ we obtain:

4.15 $$\Theta(X)\Theta(X^{-p}) \equiv 1 + X + \ldots + X^{N-1} + pS(X) \pmod{X^N - 1}$$

where again $S(X)$ is the sum of one or more positive terms whose coefficients total m.

Now notice that the left hand products of 4.8.1 and 4.8.2 are equal to the left hand products of 4.14 and 4.15 (i.e. $\Theta(X)\Theta(X^{-1})\Theta(X^p)\Theta(X^{-p}) = \Theta(X^p)\Theta(X^{-1})\Theta(X)\Theta(X^{-p})$ and now letting

$$T(X) = 1 + X + \ldots + X^{N-1}$$

the equality of the right hand products yields:

4.16 $$T^2(X) + 2nT(X) + n^2 \equiv T^2(X) + p\big(R(X) + S(X)\big)T(X) + p^2R(X)S(X) \pmod{X^N - 1}$$

and since for any i,

$$X^i(T(X)) \equiv T(X) \pmod{X^N - 1}$$

we see that:

$$R(X)T(X) \equiv S(X)T(X) \equiv mT(X),$$

and hence 4.16 simplifies to

4.17 $$n^2 \equiv p^2\left(R(X)S(X)\right) \pmod{X^N - 1}$$

But 4.17 implies that R(X) and p(X) consist of but a single term each such that the product of factors involving X only are congruent to 0 (mod $X^N - 1$). Hence we have:

4.18 $$R(X) \equiv mX^s, \text{ and } S(X) \equiv mX^{N-s} \pmod{X^N - 1}$$

now substituting back into 4.14 we have

4.19 $$\theta(X^p)\theta(X^{-1}) \equiv T(X) + nX^s \pmod{X^N - 1}$$

and now multiplying by $\theta(X)$ and using 4.8.1 we have:

4.20 $$\theta(X^p)\cdot(n+T(X)) \equiv \theta(X)\cdot(T(X)+nX^s) \pmod{X^N - 1}$$

and again using the fact that

$$X^iT(X) \equiv T(X)$$

we find in succession:

4.21 $$n\theta(X^p)+(n+1)T(X)) \equiv (n+1)\cdot(T(X)) + \theta(X)nX^s \pmod{X^N -1}$$

hence

4.22 $$\theta(X^p) \equiv X^s\theta(X) \text{ or } \sum_{i=0}^{n} X^{pa_i} \equiv \sum_{i=0}^{n} X^{a_i+s} \pmod{X^N - 1}$$

so p is a multiplier.

Theorem 6: (Mann's Theorem 1) [5] Suppose there is a difference set modulo N. If any multiplier t is of even order modulo a prime factor q of N, then n must be a square.

Proof: Let t be a multiplier, and let t have order 2f modulo q. Then

6.1 $$t^f \equiv -1 \pmod{q}$$

Using the function $\theta(X)$ defined in theorem 4, and applying theorem 5 we have:

6.2 $$\theta(X^{t^f}) \equiv X^s\theta(X) \pmod{X^N - 1}$$

for some s. Substituting a primitive q^{th} root of unity ζ for X, and using 6.1, we have:

6.3 $$\theta(\zeta^{t^f}) = \theta(\zeta^{-1}) = \zeta^s\theta(\zeta)$$

(Note that because ζ is a root of unity, the congruence becomes an equality).

Since N is odd the prime q must be odd and hence there exists an r such that

6.4 $$2r \equiv s \pmod{q}$$

Now multiplying 6.3 by $\theta(\zeta)$ we have:

6.5 $$\theta(\zeta)\theta(\zeta^{-1}) = \zeta^s(\theta(\zeta)^2) \equiv \zeta^{2r}\theta(\zeta)^2 = (\zeta^r\theta(\zeta))^2$$

and by theorem 5

6.6 $$(\zeta^r\theta(\zeta))^2 = n + 1 + \zeta + \zeta^2 + \ldots + \zeta^{N-1} = n$$

since $1 + \zeta + \ldots + \zeta^{q-1} = 0$ and q divides N. Hence we have

6.7 $$(\zeta^r\theta(\zeta))^2 = n$$

Now in the field $\mathcal{F}(\zeta)$ generated by ζ over the rational numbers, the only quadratic subfield is $\mathcal{F}(\sqrt{\pm q})$ and hence either n is a square, or $n = a^2q$. But q cannot divide n, as q divides N, hence n must be a square.

Corollary 6.1: (Mann's Corollary 2) [5] Suppose there is a difference set modulo N, p is a multiplier, and that q is a

prime divisor of N. If p is a quadratic non-residue (mod q), then n must be a square.

Suppose the order α of p is odd. Then we have

6.6.1 $p^{\alpha} \equiv 1 \pmod{q}$

6.6.2 $p^{\alpha+1} \equiv p \pmod{q}$

and since α is odd, we can write: $p^{2\beta} \equiv p \pmod{q}$

hence p is a quadratic residue (mod q) if p is of odd order modulo q, and it follows that if p is a quadratic non-residue (mod q), then p is of even order, and by theorem 6, n must be a square.

Theorem 7: (Mann's theorem 2) [5] The prime p is a multiplier if and only if

7.1 $$\theta(X)^p \equiv X^s \theta(X) \qquad \text{modd } (p, X^N - 1)$$

Proof: (I) The "if" part is obvious in view of theorem 5.

(II) By theorem 5 we have ;

7.2 $$\theta(X)^p \equiv X^s\theta(X) \qquad \text{modd } (p, X^N - 1)$$

implies

7.3 $$\theta(X^p) \equiv X^s\theta(X) \qquad \text{modd } (p, X^N - 1)$$

Since $\theta(X^p)$ and $X^s\theta(X)$ are polynomials whose coefficients are either 1 or 0, it follows that

7.4 $$\theta(X^p) \equiv X^s\theta(X) \qquad \text{mod } (X^N - 1)$$

and hence p is a multiplier

Definition 5: If p is a prime multiplier and if p does not divide n, then p will be called an extraneous multiplier.

Theorem 8: (Mann's Theorem 2) [5] If p is an extraneous multiplier then

8.1 $$\theta(X)^{p-1} \equiv X^s \qquad \text{mod}_d(p, X^N - 1)$$

if $n + 1 \not\equiv 0 \pmod{p}$, and

8.2 $$\theta(X)^{p-1} \equiv X^s - T(X) \qquad \text{mod}_d(p, X^N - 1)$$

if $n+1 \equiv 0 \pmod{p}$ (where T(X) is the polynomial defined in theorem 5.)

Proof: Since p is a multiplier, we have by theorem 7

8.3 $$\theta(X)^p \equiv X^s\theta(X) \qquad \text{mod}_d(p, X^N - 1)$$

Now multiply 8.3 by $\theta(X^{-1})$ to obtain

8.4 $$\theta(X)^{p-1}(n + T(X)) \equiv X^s(n + T(X)) \qquad \text{mod}_d(p, X^N - 1)$$

and multiplying out the left side and reducing mod $(X^N - 1)$ we obtain,

8.5 $$n\theta(X)^{p-1} + (n + 1)^{p-1}T(X) \equiv X^s(n + T(X)) \qquad \text{mod}_d(p, X^N - 1)$$

since the product of any polynomial F(X) with T(X), reduced modulo $X^N - 1$, equals T(X) times the sum of the coefficients of F(X).

(I) If $n + 1 \not\equiv 0 \pmod{p}$, then $(n + 1)^{p-1} \equiv 1 \pmod{p}$, as $p - 1 = \phi(p)$.

(II) If $n + 1 \equiv 0 \pmod{p}$, then $n \equiv -1 \pmod{p}$. Also

$$X^sT(X) \equiv T(X) \qquad \text{mod } (X^N - 1)$$

Hence if

$$n + 1 \not\equiv 0 \pmod{p}$$

8.5 yields 8.1 $$\theta(X)^{p-1} \equiv X^s \qquad \text{mod}_d(p, X^N - 1)$$

and if

$$n + 1 \equiv 0 \pmod{p}$$

8.5 yields 8.2

$$-\theta(X)^{p-1} + 0 \equiv -X^s + T(X)$$

or

$$\theta(X)^{p-1} \equiv X^s - T(X) \qquad \text{modd}(p, X^N - 1)$$

and the theorem is proved

Corollary 8.1: (Mann's Corollary 1) [5] If 2 is a multiplier for a difference set (mod N), then n must be even..

Proof: Deny, then by theorem 8, either

8.1.1

$$\theta(X) \equiv X^s \qquad \text{modd}(2, X^N - 1)$$

or

8.1.2 $$\theta(X) \equiv X^s + T(X) \qquad \text{modd}(2, X^N - 1)$$

both of which are impossible since the coefficients of $\theta(X)$ are all 1, and $\theta(X)$ has n + 1 terms, not more than 1 of which is congruent to X^s modulo $(X^N - 1)$.

Corollary 8.2: (Mann's Corollary 2) [5] If 3 is a multiplier for a difference set (mod N) then $n \equiv 0 \pmod 3$.

Proof: Deny, then by theorem 8 either

8.2.1

$$\theta(X)^2 \equiv X^s \qquad \text{modd}(3, X^N - 1)$$

or

8.2.2 $$\theta(X)^2 \equiv X^s - T(X) \qquad \text{modd}(3, X^N - 1)$$

But X^m occurs in $\theta(X)^2$ if $m = a_i + a_j$ and it occurs exactly twice if $i \neq j$ and exactly once if $i = j$. Also, X^m does not occur for exactly $1/2[n(n + 1)]$ values of m. In particular $\theta(X)^2$ will contain at least two distinct powers of X, say $2X^{2a_1}$ and $2X^{2a_2}$ and since $a_i + a_j = a_j + a_i$, $\theta(X)^2$ cannot

contain N - 1 powers of X. Furthermore, no coefficient of $(X)^2$ is congruent to 0 (mod 3), hence both 8.2.1 and 8.2.2 are impossible.

Definition 6: Let $\{a_i\}_{i=0}^{n}$ be a difference set, and let t be any multiplier. then if

$$\{ta_i\}_{i=0}^{n} \equiv \{a_i\}_{i=0}^{n} \pmod{N}$$

in some order, $\{a_i\}_{i=0}^{n}$ will be called a fixed difference set. In the following theorem the proof, which is a geometric one, is omitted.

Theorem 9: (Hall's Corollary 4.11) If there is a difference set (mod N) then there is a fixed difference set (mod N).

Theorem 10: (Mann and Evans' Theorem 5) [2] Let $\{a_i\}_{i=0}^{n}$ be a fixed difference set (mod N). Then

I) 0 is contained in the set $\{a_i\}_{i=0}^{n}$ if $n \equiv 0 \pmod 3$

II) 0 is not contained in the set $\{a_i\}_{i=0}^{n}$ if $n \equiv 2 \pmod 3$.

Proof: n is a multiplier, and if N' is any divisor of N, then the order of n (mod N') is either 3 or 1. But if $n \equiv 1 \pmod{N'}$ then

$$N = n^2 + n + 1 \equiv 3 \pmod{N'},$$

so if N' is a factor of N, we must have N'= 3, therefore if $n \equiv 0$ or 2 (mod 3), N' is of order 3 modulo any factor of N. Now let a be any element of the fixed difference set $\{a_i\}_{i=0}^{n}$ different from 0. Then

$$n^k a \equiv a \pmod{N}$$

is possible only if $k \equiv 0 \pmod 3$, since n is of order 3. Hence upon multiplication by n, the non-zero residues are permuted in cycles of length 3 and the theorem follows.

Theorem 11: (Mann's Theorem 4) [5] If t_1, t_2, t_3, t_4 are

all multipliers for a difference set (mod N) and if

11.1 $(t_1 - t_2) = (t_3 - t_4)$

then

11.2 $(t_1 - t_2)(t_1 - t_3) \equiv 0 \pmod{N}$

Proof: Let $\{a_i\}_{i=0}^{n}$ be a difference set fixed under all multipliers, and then for any a in this set, t_1a, t_2a, t_3a, t_4a are also in this set. Also by 11.1 we have

11.3 $t_1a - t_2a \equiv t_3a - t_4a$

but since each non-zero residue appears as a difference only once, then either

11.4 $t_1a \equiv t_2a \pmod{N}$ or,

11.5 $t_1a \equiv t_3a \pmod{N}$

Since this is true for every a in $\{a_i\}_{1=0}^{n}$, we have for every integer m,

11.6 $(t_1 - t_2)(t_1 - t_3)m \equiv 0 \pmod{N}$,

and the theorem is proved.

Corollary 11.1: (Mann and Evans' Corollary 2.1) [2] Let p_1, p_2, p_3, q be prime divisors of n such that

(1) $q - p_1^{\alpha_1} = p_2^{\alpha_2} - p_3^{\alpha_3}$

where $\alpha_i \geq 0$, $i = 1,2,3$

(2) $p_1, p_2 \neq q$

(3) $p_i^{\alpha_i} < 2q$ for $i = 1,2$

Then there is no difference set (mod N)

Proof: Assume there is a difference set (mod N), then by

theorem 5, and the fact that the product of two multipliers is a multiplier, $p_i^{\alpha_i}$, $i = 1,2,3$ and q are multipliers. By theorem 11, we have

10.1.1 $(q - p_1^{\alpha_1})(q - p_2^{\alpha_2}) \equiv 0 \pmod{n^2 + n + 1}$.

But

10.1.2 $|(q - p_1^{\alpha_1})(q - p_2^{\alpha_2})| < 4q^2$ and $\neq 0$

(since $p_i^{\alpha_i} < 2q$, $i = 1,2$ and $p_1, p_2 \neq q$ by hypothesis)

Also $n > 2q$ (since $p_1 q$ divides n) and so

10.1.3 $|(q - p_1^{\alpha_1})(q - p_2^{\alpha_2})|$ $n^2 + n + 1$ and $\neq 0$

Thus 10.1.1 and 10.1.3 are contradictory, whence the theorem.

Theorem 12: If p is a prime factor of N, and $y \equiv -3 \pmod{p}$ then y is a quadratic residue (mod p).

Proof: If p is a prime factor of N, then

12.1 $n^2 + n + 1 \equiv 0 \pmod{p}$

Now 12.1 is a special case of the general quadratic congruence

12.2 $ax^2 + bx + c \equiv 0 \pmod{p}$

with a, b, c, all = 1, hence if we investigate the possible solutions of

$$x^2 + x + 1 \equiv 0 \pmod{p},$$

we will have some knowledge of what kind of prime factors N has.

It is known in number theory that the solution of the quadratic congruence 12.2 is equivalent to the solution of the

pair of congruences

12.3 $u^2 \equiv b^2 - 4ac \pmod{p}$

and

12.4 $2ax \equiv u - b \pmod{p}$,

Since 12.4 has a solution only if 12.3 has a solution, we need consider only 12.3 and since a,b,c all = 1, we find 12.3 becomes

12.5 $u^2 \equiv -3 \pmod{p}$

Hence if p divides N, then 12.5 has a solution, and - 3 is a quadratic residue modulo p.

Definition 7: Let q be a prime factor of N. .

(1) We shall say that q is a factor of type I if there is some multiplier t (mod N) such that the order of t (mod N) is greater than the order of t (mod q).

(2) We shall say that q is of type II if the order of every multiplier (mod q) is equal to its order (mod N).

Remark 1: No divisor of zero (mod N) can be a multiplier, since if a difference set $\{a_i\}_{i=0}^{n}$ be multiplied by a divisor of zero, at least one of the differences $\{a_i - a_j\}_{\substack{i,j=0 \\ i \neq j}}^{n}$ will be carried into zero, and hence every prime factor of N is either of type I or type II.

Theorem 13: (Ostrom's Theorem 1) Suppose that there is a difference set (mod N) and that N has a prime factor q of type I, and let t be the multiplier whose order (mod q) and (mod N) were considered. Let α be the order of t (mod q), and let $N_1 = (t^{\alpha} - 1, N)$. Then (a) q divides $N_1 \neq N$, (b) N_1

is of the form $n_1^2 + n_1 + 1$, (c) there is a difference set (mod N_1), (d) every multiplier of the difference sets (mod N) is a multiplier for the difference sets (mod N_1).

Proof: This theorem is essentially restatement of Hall's theorem 4.6, with some minor modifications in terminology.

Corollary 13.1: (Ostrom's Corollary 1) Suppose that $n = m^r$, where $(r,3) = 1$ and there is a difference set (mod N) where $N = n^2 + n + 1$. Then there is a difference set (mod $N_1 = m^2 + m + 1$) and every multiplier (mod N) is a multiplier (mod N_1).

Proof: Let $(m - 1, N) = N'$. Then

13.1.1 $m \equiv 1 \pmod{N'}$

and

13.1.2 $N = m^{2r} + m^r + 1 \equiv m^2 + m + 1 \equiv 3 \pmod{N'}$

Hence by 13.1.1 and 13.1.2, $N' = 1$ or 3 and if $N' = 3$, then

13.1.3 $m^2 + m + 1 \equiv 0 \pmod{N'}$

It can be verified by testing all the residues (mod 9) that in no case is $n^2 + n + 1 \equiv 0 \pmod 9$. Hence

13.1.4 $((m^3 - 1),(m^{2r} + m^r + 1) = m^2 + m + 1$

if $(r,3) = 1$

Remark 2: If $n = m^2$, and if there is no difference set (mod $m^2 + m + 1$) then there is no difference set (mod n^2+n+1). Note that remark 2 can be used to eliminate a possible value of n for a difference set when n is a square, and as a consequence, theorem 6 fails.

Theorem 14: (Ostrom's Theorem 2) If N contains a prime factor q of type II, the multipliers form a cyclic multi-

plicative group.

Proof: The product of two multipliers is a multiplier. Obviously the multipliers form a group. Let the multipliers be reduced (mod q). Since q is prime, the images of the multipliers in the residue system (mod q) form a cyclic group. We shall now show two distinct multipliers t_1 and t_2 have different images in the residue system (mod q). Suppose that $t_1 \equiv t_2 \pmod{q}$. Since the multipliers form a group, we may write:

14.1 $t_2 \equiv t_1 t_3 \pmod{N}$

(Where t_3 is a multiplier). Hence

14.2 $t_1 \equiv t_2 \equiv t_1 t_3 \pmod{q}$

and

14.3 $t_1(t_3 - 1) \equiv 0 \pmod{q}$

Now $t_x \not\equiv 0 \pmod{q}$ as a divisor of zero cannot be a multiplier. But q is prime, hence

14.4 $(t_3 - 1) \equiv 0 \pmod{q}$

Since q is a prime factor of type II, 14.4 implies that

14.5 $(t_3 - 1) \equiv 0 \pmod{N}$

Hence the mapping of the multipliers is 1——1, and the multipliers form a cyclic group (mod N).

Theorem 15: (Ostrom's Theorem 3) Suppose that

(1) there is a difference set mod $N = n^2 + n + 1$,

(2) $N = q_1 q_2 \cdots q_k$, where q_i is prime ($i = 1,2,\ldots,k$),

(3) n is not a square

(4) for some i, q_i is of type II;

then the order S of the group of multipliers is odd and

divides $\phi(q_i) = q_i - 1$.

Proof: If S is even, the order of the primitive multiplier is even and n must be a square. The order of any non-zero residue mod q_i divides $\phi(q_i)$. If q_i is of type II, the order of every multiplier mod q_i is the same as its order mod N.

Theorem 16: (Ostrom's Theorem 3.1) If the hypotheses of of theorem 3 are valid and

(5) q_i is of type II for $i = 1,2,\ldots,k$,

(6) $n + 1 \equiv 0 \pmod 3$,

then S divides n + 1,

Proof: By theorem 10 zero is not contained in the difference set fixed under all multipliers if $n + 1 \equiv 0 \pmod 3$. Let t be the primitive multiplier. Then (for any number $a \not\equiv 0$) if a is in the fixed difference set, $a, at,\ldots,at^{s-1}$ are all incongruent mod N and all included in the fixed difference set. The n + 1 numbers in this fixed set therefore occur in subsets of S each.

Theorem 17: (Ostrom's Theorem 3.2) If (1), (2), (3), (5) of theorems 15 and 16 are all satisifed and $n \equiv 0 \pmod 3$ then S divides n.

Proof: By theorem 10 zero is contained in the fixed difference set if $n \equiv 0 \pmod 3$. As in Theorem 16, the n non-zero numbers in the fixed difference set occur in subsets of S each.

Remark:3: If $n - 1 \equiv 0 \pmod 3$, $N \equiv 0 \pmod 3$ and 3 is a factor of type I.

Theorem 18: (Mann and Evans' Theorem 6) [2] Let t be a multiplier of a difference set (mod N) such that

$(t - 1, N) = N_1 \neq 1$

and $N = N_1 N_2$.

Then there is a difference set (mod N_1) and if $\{b_j N_2\}$ represents the set of multiples of N_2 in a fixed difference set $\{a_i\}_{i=0}^{n}$ (mod N), then the set $\{b_j\}_{i=0}^{n_1}$ is a difference set (mod N_1).

Proof: Let $\{a_i\}_{i=0}^{n}$ be a fixed set (mod N) and let a_i, a_j be any two residues of $\{a_i\}_{i=0}^{n}$ such that

18.1 $a_i - a_j \equiv 0 \pmod{N_2}$

then

18.2 $(t - 1)(a_i - a_j) \equiv 0 \pmod{N}$

or

18.3 $ta_i - ta_j \equiv a_i - a_j \pmod{N}$

By the definition of a fixed set, ta_i and ta_j are residues of $\{a_i\}_{i=0}^{n}$. From the defining property of a difference set, 18.3 yields

18.4 $ta_i \equiv a_i$ and $ta_j \equiv a_j \pmod{N}$

and since by hypothesis $(t - 1, N) = N_1$, 18.4 implies

18.5 $a_i, a_j \equiv 0 \pmod{N_2}$.

Hence we have

18.6 $a_i - a_j \equiv 0 \pmod{N_2}$

if and only if $a_i, a_j \equiv 0 \pmod{N_2}$. Now let $\{b_j N_2\}$ be the set of all residues of $\{a_i\}_{i=0}^{n}$ which are multiples of N_2. By 18.6 and the definition of a difference set, the congruences

18.7 $b_i N_2 - b_j N_2 = kN_2 \pmod{N}$

for $k = 1,2,\ldots N_1 - 1$ must be uniquely satisfied by some b_iN_2, b_jN_2 in $\{b_jN_2\}$. Hence the congruences

18.8 $\quad b_i - b_j \equiv k \pmod{N_1}$

for $k = 1,2,\ldots,N_1 - 1$ are satisfied uniquely, and hence there is a difference set (mod N_1) and $\{b_j\}_{i=0}^{n_1}$ is a difference set (mod N_1)

Theorem 19: (Ostrom's Theorem 3.3) Suppose that:

(1) there is a difference set mod N,

(2) $N = N_1N_2$ (N_1 and N_2 not necessarily prime),

(3) every factor of N_2 is of type II with respect to N,

(4) $(t^{\alpha} - 1, N) = N_1$, where $\alpha < S$ and t is a multiplier;

then N_1 is of the form $n_1^2 + n_1 + 1$ and S divides $n \mp n_1$.

Proof: By theorem 13, there is a difference set mod N_1 and $N_1 = n_1^2 + n_1 + 1$. By theorem 18, there are $n_1 + 1$ multiples of N_2 in the fixed difference set. If a is any residue mod N which is not a multiple of N_2, let β be the least power of the multiplier t such that $at^{\beta} \equiv a \pmod{N}$. Then $a(t^{\beta} - 1) \equiv 0 \pmod{N = N_1N_2}$. Hence $t^{\beta} - 1 \equiv 0$ mod some factor of N_2. Since all factors of N_2 are of type II with respect to N, $\beta = S$. Thus the $n - n_1$ residues in the fixed difference set which are non-multiples of N_2 occur in sets $a, at, \ldots, at^{S-1}$ of S each, and S divides $n - n_1$.

The remaining results below proved valuable aids in eliminating composite values of n for difference set.

Remark 4: 2 is a quadratic residue only for primes of the form $8k \pm 1$.

Proof: It is well known in number theory that $(2/p) = (-1)^{(p^2 - 1)/8}$ from which remark 3 follows (where (2/p) is Legendre's symbol).

Remark 5: (Mann and Evans' Corollary 3.2, test "b") [2] Suppose there is a difference set (mod N). If $n \equiv 4,6 \pmod 8$, then n must be a square.

Proof: If $n \equiv 6 \pmod 8$, there is no difference set for then n cannot be a square. If $n \equiv 4 \pmod 8$, then $n \equiv 0$ mod 2 and hence 2 is a multiplier. Now (2/N) = -1 since if $n \equiv 4 \pmod 8$, then $N \equiv 5 \pmod 8$ hence there exists at least one prime factor q of N, such that $q \not\equiv \pm 1 \pmod 8$.

Remark:6: (Mann and Evans Corollary 3.3, test "c") [2] Suppose there is a difference set (mod N). If $n \equiv 1, 2 \pmod 4$ and $p \equiv 3 \pmod 4$, where p is a prime factor of n, then n must be a square.

Proof: $(N/p) = (n^2+n+1/p) = 1$

since p divides n. For $n \equiv 1$ or $2 \pmod 4$, $N \equiv 3 \pmod 4$ and since $p \equiv 3 \pmod 4$ by hypothesis, from the quadratic reciprocity law, (p/N) = -(N/p), Hence (p/N) = -1 and so for some prime divisor q of N, (p/q) = -1, and so n must be a square.

Remarks 4 and 5 are special cases of corollary 6.1 of theorem 6.

Remark 7: (Mann and Evans' Test "a") [2] By corollary 11.1 if any value of n has among its factors any of the combination listed below, then there is no difference set (mod N).

2,3
2,5
2,7
2,11
2,13
2,17
2,19
2,23
2,29
2,31
2,47
2,61
2,67
2,71
2,79
2,97
2,113
2,127
2,131
2,191
2,193
2,241
2,257
2,263
2,271
2,383
2,449
2,509
2,769
3,5
3,7
3,11
3,13
3,17
3,19
3,29
3,53
3,73
3,79
3,83
3,89
3,107
3,163
3,241
3,251
3,269
3,487
5,7
5,11
5,13
5,29
5,101
5,149
7,13
7,43
7,97
11,131
19,37
31,61
7,11,17

CHAPTER III

ELIMINATION OF ALL COMPOSITE NUMBERS LESS THAN 2501

In this chapter, we show that no difference set exists for n less than 2501 and for n not a power of a prime. The theorems listed in chapter II are used (sometimes in combinations) to eliminate the individual cases. The values of n will be considered in two main categories, even and odd.

I (n even) using corollary 11.1(corollary 2.1, and test "a" Mann and Evans) [2], we eliminate the following values of n which have the incompatible factors according to test "a". (Note: Since n is even, only factors of n other than 2 are listed.)

n	factor	n	factor
1600	5	1656	3
1602	3	1660	5
1606	11	1662	3
1608	3	1664	13
1610	5	1666	7
1612	13	1668	3
1614	3	1670	5
1620	3	1672	11
1624	7	1674	3
1626	3	1680	3
1628	11	1682	29
1630	5	1686	3
1632	3	1690	5
1634	19	1692	3
1638	3	1694	7
1640	5	1698	3
1644	3	1700	5
1650	3	1702	23
1652	7	1704	3

n	factor	n	factor
1708	7	1850	5
1710	3	1854	3
1716	3	1856	29
1720	5	1860	3
1722	3	1862	7
1728	3	1866	3
1730	5	1870	5
1734	3	1872	3
1736	7	1874	47
1738	11	1876	7
1740	3	1878	3
1742	13	1880	5
1746	3	1884	3
1748	19	1886	23
1750	5	1890	3
1752	3	1892	11
1758	3	1896	3
1760	5	1898	13
1764	3	1900	5
1768	17	1902	3
1770	3	1904	7
1776	3	1908	3
1778	7	1910	5
1780	5	1914	3
1782	3	1918	7
1786	19	1920	3
1788	3	1922	31
1790	5	1924	13
1792	7	1926	3
1794	3	1928	241
1796	449	1930	5
1798	29	1932	3
1800	3	1936	11
1802	17	1938	3
1804	11	1940	5
1806	3	1944	3
1808	113	1946	7
1810	5	1950	3
1812	3	1952	61
1818	3	1954	79
1820	5	1956	3
1824	3	1958	11
1826	11	1960	5
1830	3	1962	3
1834	7	1968	3
1836	3	1970	5
1840	5	1972	17
1842	3	1974	3
1846	13	1976	13
1848	3	1978	23

n	factor	n	factor
1980	3	2114	7
1984	31	2116	23
1986	3	2118	3
1988	7	2120	5
1990	5	2124	3
1992	3	2128	7
1998	3	2130	3
2000	5	2132	13
2002	7	2134	11
2004	3	2136	3
2006	17	2140	5
2010	3	2142	3
2014	19	2144	67
2016	3	2146	29
2020	5	2148	3
2022	3	2150	5
2024	11	2154	3
2028	3	2156	7
2030	5	2158	13
2032	127	2160	3
2034	3	2162	23
2036	509	2166	3
2040	3	2168	271
2044	7	2170	5
2046	3	2172	3
2050	5	2176	17
2052	3	2178	3
2054	13	2180	5
2056	257	2184	3
2058	3	2190	3
2060	5	2196	3
2062	47	2198	7
2064	3	2200	5
2068	11	2202	3
2070	3	2204	19
2072	7	2208	3
2074	17	2210	5
2076	3	2212	7
2080	5	2214	3
2082	3	2220	3
2086	7	2222	11
2088	3	2226	3
2090	5	2230	5
2094	3	2232	3
2096	131	2236	13
2100	3	2238	3
2104	263	2240	7
2106	3	2242	19
2108	17	2244	3
2110	5	2250	3
2112	3	2254	7

n	factor
2256	3
2260	5
2262	3
2266	11
2268	3
2270	5
2272	71
2274	3
2278	17
2280	3
2282	7
2286	3
2288	11
2290	5
2292	3
2294	31
2296	7
2298	3
2300	5
2304	3
2310	3
2312	17
2314	13
2316	3
2318	19
2320	5
2322	3
2324	7
2328	3
2332	11
2334	3
2338	7
2340	3
2344	47
2346	3
2350	5
2352	3
2354	11
2356	13
2358	3
2360	5
2364	3
2366	7
2370	3
2376	3
2378	29
2380	7
2382	3
2388	3
2390	5
2392	23
2394	3
2398	11
2400	3
2406	3
2408	7
2410	5
2412	3
2414	17
2418	3
2420	5
2422	7
2424	3
2428	79
2430	3
2432	19
2434	13
2436	3
2438	23
2440	5
2442	3
2448	3
2450	5
2454	3
2460	3
2464	7
2466	3
2470	19
2472	3
2478	3
2480	5
2482	17
2484	3
2486	11
2490	3
2492	7
2494	29
2496	3
2500	5

To eliminate cases using tests other than corallary 11.1 above, the prime decomposition of N is either desireable or necessary, hence all remaining numbers were factored using Lehmer's "Factor Table for the First Ten Million". We next apply Theorem 6 (Mann's Theorem 1); we apply Remark 4 to determine whether or not 2 is a quadratic non-residue modulo a factor of N, and the following list of numbers is thus eliminated. (Note: by Remark 4 we know that 2 is a quadratic residue only for primes of the form $8K \pm 1$).

n	Prime factors of N Modulo 8	n	Prime factors of N Modulo 8
1604	3,7	2384	7,5,3
1622	3,3,5	2396	7,3
1636	3,3	2426	7,5,5
1646	3	2444	3,7
1676	5	2462	3
1688	3,3	2468	7,7,5,1
1718	3		
1724	7,3		
1766	7,5		
1774	3		
1814	3		
1838	7,3,7		
1844	7,3		
1934	7,5		
1964	7,3,1		
1982	3		
2012	7,3		
2042	3,5		
2078	3,1		
2084	5,1		
2126	5,7		
2186	7,7,3,5		
2192	3,3		
2216	7,5,3		
2228	7,3		
2234	3,3,7		
2246	5,7		
2306	3,3,7		
2342	7,5,1		
2348	3,3,5		
2372	5		

Next, the remaining numbers were checked to see if in any case there is a factor of n which is of even order mudulo a factor of N. The following list was eliminated by this test. In each case below, 2 is a factor of n, 3 is a factor of N and 2 is of even order modulo 3.

n	n	n
1618	1912	2308
1642	1942	2326
1678	1948	2368
1684	1996	2374
1696	2008	2386
1714	2026	2404
1726	2038	2416
1744	2092	2446
1756	2098	2452
1762	2126	2458
1774	2152	2476
1822	2182	2488
1828	2188	
1852	2194	
1858	2218	
1864	2224	
1882	2248	
1906	2302	

In each case below, 2 is a factor of n, 13 is a factor of N and 2 is of even order modulo 13.

n	n	n
1654	1888	2206
1706	1894	2252
1712	1966	2258
1732	2018	2284
1784	2102	2330
1816	2122	2336
1868	2174	2362

The remaining even numbers were eliminated by using one of Ostrom's Theorems, or a combination thereof. The remaining numbers and details of eliminating each or a possible difference set value are listed below. It will be well to keep

the following things in mind in using Ostrom's Theorems 3.1 and 3.2.

(1) We will assume that there is a difference set in every case.

(2) Wherever there is a factor of type II, the multipliers form a cyclic group, that is, the group can be generated by at least one of its elements, by Ostrom's Theorem 2.

(3) We will let S denote the order of the group of multipliers.

(4) The order of any element in a group divides the order of the group.

(5) We can, without loss of generality, assume n is not a square, by Ostrom's Theorem 1, hence the order of any multiplier must be odd.

For n = 1616, 1658, 1832, 1994, 2138, 2264, 2402, 2456, 2474, 2498, N is a prime, and hence a factor of type II. Also, since N is prime, and n even Ostrom's theorem 3.1 must apply, hence S divides n + 1. (Note: if $(n - 1) \equiv 0 \pmod 3$, then 3 divides N).

For n = 1616, 1658, 1832, 1994, 2138, 2264, 2402, 2456, 2474, 2498 we find that theorem 3.1 applies, and in every case the order of 2 is not a factor of n + 1, hence a contradiction and no difference set can exist. We list the details below:

n	Multi-plier	N	Theorem 3.1 or 3.2	Contradiction
1616	2	2613073	$n + 1 \equiv 0(\text{Mod } 3)$	$2^{1617} \not\equiv 1(\text{Mod } N)$
1658	2	2750623	$n + 1 \equiv 0(\text{Mod } 3)$	$2^{1659} \not\equiv 1(\text{Mod } N)$
1832	2	3358057	$n + 1 \equiv 0(\text{Mod } 3)$	$2^{1833} \not\equiv 1(\text{Mod } N)$
1994	2	3978031	$n + 1 \equiv 0(\text{Mod } 3)$	$2^{1995} \not\equiv 1(\text{Mod } N)$
2138	2	4573183	$n + 1 \equiv 0(\text{Mod } 3)$	$2^{2139} \not\equiv 1(\text{Mod } N)$
2264	2	5127961	$n + 1 \equiv 0(\text{Mod } 3)$	$2^{2265} \not\equiv 1(\text{Mod } N)$
2402	2	5772007	$n + 1 \equiv 0(\text{Mod } 3)$	$2^{2403} \not\equiv 1(\text{Mod } N)$
2456	2	6034393	$n + 1 \equiv 0(\text{Mod } 3)$	$2^{2457} \not\equiv 1(\text{Mod } N)$
2474	2	6123151	$n + 1 \equiv 0(\text{Mod } 3)$	$2^{2475} \not\equiv 1(\text{Mod } N)$
2498	2	6242503	$n + 1 \equiv 0(\text{Mod } 3)$	$2^{2499} \not\equiv 1(\text{Mod } N)$

For n = 1754, we have = 3078271 = 7·439753. 7 is a factor of type I, and applying Ostroms theorem 1, we see that all conditions of the theorem are satisfied, so we apply Ostrom's theorem 3.3. Now 439753 is not of the form $n_1^2 + n_1 + 1$, hence by theorem 1, it must be a factor of type II. By theorem 3.3, S divides $n - n_1 = 1754 - 2 = 1752$, also by theorem 3 S is odd, so S divides 219, as 1754 = =219·8. We find the order of 2 is>219, hence no difference set for n = 1754.

For n = 2066, we have N= 4270423 = 1423·3001. Neither factor of N is of the form $n_1^2 + n_1 + 1$, hence neither can be of type I, so both must be of type II, by Ostrom's theorem I. Now we are in a position to apply Ostrom's theorem 3, and theorem 3.1 (since $n + 1 = 2027 \equiv 0(\text{mod } 3)$) we find S must divide 3, which is impossible as the order of 2 is greater

than 3, and 2 is in the group of multipliers.

For n = 1648, 1772, 1916, 2164 N has a factor of 31. Now since there is a difference set modulo 31, every multiplier or n should be a multiplier for 31 by Ostrom's theorem 1, but 2 is not a multiplier for 31, hence a contradiction, and no difference set exists.

This completely eliminates all the even composite numbers up to 2500 as possible values for difference sets, except of course $2^{11} = 2048$.

II (n odd) using corollary 11.1(corollary 2.1) and test "a" (Mann and Evans) [2] we eliminate the following list of values of n having incompatible pairs of factors.

n	factors	n	factors
1599	3,13	1833	3,13
1605	3,5,107	1845	3,5
1617	3,7,11	1855	5,7,53
1625	5,13	1869	3,7,89
1635	3,5	1875	3,5
1645	5,7	1881	3,11,19
1653	3,19,29	1885	5,13,29
1659	3,7,79	1887	3,17,37
1665	3,5,37	1891	31,61
1677	3,13,43	1905	3,5
1683	3,11,17	1911	3,7,13
1695	3,5	1925	5,7,11
1701	3,7	1935	3,5,43
1705	5,11,31	1947	3,11
1715	5,7	1953	3,7,31
1725	3,5	1965	3,5,131
1729	7,13,19	1971	3,73
1743	3,7,83	1989	3,13,17
1749	3,11,53	1995	3,5,7,19
1755	3,5,13	2001	3,29
1767	3,19,31	2013	3,11,61
1785	3,5,7,17	2015	5,13,31
1815	3,5,11	2025	3,5
1827	3,7,29	2035	5,11,37

n	factors	n	factors
2037	3,7,97	2301	3,13
2055	3,5	2325	3,5,31
2065	5,7	2337	3,19
2067	3,13,53	2343	3,11
2079	3,7,11	2345	5,7
2085	3,5	2349	3,29
2091	3,17	2355	3,5
2093	7,13	2365	5,11,43
2107	7,43	2373	3,7
2109	3,19,37	2379	3,13,61
2115	3,5	2385	3,5,53
2121	3,7,101	2397	3,17
2133	3,79	2401	7
2135	5,7,61	2403	3,89
2145	3,5,11,13	2405	5,13,37
2163	3,7	2409	3,11,73
2169	3,241	2415	3,5,7
2175	3,5,29	2421	3,269
2187	3	2445	3,5,163
2193	3,17,43	2451	3,19,43
2197	13	2457	3,7,13
2205	3,5,7	2465	5,17,29
2211	3,11	2475	3,5,11
2223	3,13,19	2485	5,7
2235	3,5,149	2499	3,7,17
2247	3,7,107	2505	3,5
2255	5,11		
2259	3,251		
2265	3,5		
2275	5,7,13		
2277	3,11		
2289	3,7		
2295	3,5,17		

For the remaining odd numbers, we compute N and factor both N and n using Lehmer's factor tables. Next, using a table of indices for moduli up to 1000, and for primes less than 50, we eliminate all cases where a prime factor of n is of even order modulo a prime factor of N. These are listed below:

n	Factor of n	Factor of N
1603	7	79
1615	5	3

n	Factor of n	Factor of N
1623	3	331
1629	3	523
1631	7	127
1639	11	3
1641	3	19
1647	3	7
1649	17	7
1671	3	241
1673	7	13
1675	5	3
1679	73	31
1687	7	73
1689	3	7
1691	19	37
1703	13	7
1711	29	3
1713	3	43
1717	17	7
1719	3	7
1731	3	7
1735	5	3
1745	5	7
1751	17	367
1761	3	7
1763	43	673
1765	5	3
1769	29	43
1771	7	13
1773	3	7
1775	5	7
1779	3	67
1781	13	97
1791	3	967
1795	5	3
1797	3	19
1799	7	43
1803	3	7
1807	13	97
1813	7	337
1819	17	691
1821	3	193
1825	5	3
1829	31	7
1837	11	3
1839	3	37
1843	19	61
1851	3	163
1857	3	7
1859	13	307
1893	3	337
1897	7	163

n	Factor of n	Factor of N
1899	3	7
1903	11	3
1909	83	3
1915	5	3
1921	17	3
1929	3	7
1941	3	7
1943	29	241
1945	5	3
1955	5	7
1957	19	7
1961	37	457
1969	11	3
1975	5	3
1983	3	7
1985	5	13
1991	11	409
2005	5	3
2019	3	397
2031	3	523
2041	13	7
2045	5	37
2047	89	3
2051	7	127
2057	11	13
2059	29	3
2061	3	37
2095	5	3
2097	3	7
2101	11	3
2103	3	883
2119	13	37
2123	11	181
2125	5	3
2127	3	139
2139	3	7
2149	7	373
2151	3	7
2155	5	3
2165	5	7
2167	11	3
2177	7	163
2181	3	7
2185	5	3
2195	5	7
2199	3	43
2215	5	3
2217	3	607
2227	17	3
2229	3	43
2233	11	3

n	Factor of n	Factor of N
2245	5	3
2249	13	7
2253	3	19
2263	31	7
2271	3	73
2279	43	661
2283	3	37
2285	5	43
2291	79	19
2299	11	3
2305	5	3
2307	3	7
2315	5	43
2317	7	13
2319	3	7
2323	101	3
2327	13	73
2329	17	3
2335	5	3
2361	3	7
2363	17	7
2367	3	19
2375	5	7
2391	3	7
2395	5	3
2407	29	3
2425	5	3
2431	11	3
2433	3	7
2439	3	19
2449	31	67
2453	11	13
2455	5	3
2461	107	3
2479	37	13
2481	3	19
2487	3	7
2489	19	7
2491	53	3
2497	11	3
2501	61	7
2515	5	3
2517	3	7

Next, using the quadratic reciprocity law, we eliminate all cases in which--to use Legendre's symbol--$(p/q) = -1$, where p is a prime factor of n and q a prime factor of N. Since by Mann's theorem 1 if p is a quadratic non-residue modulo q,

then n is a square. The following were eliminated in this way.

n	Quadratic non-residue	Modulus
1611	179	N
1633	23	61
1643	31	1009
1655	5	1153
1661	11	394369
1727	11	1657
1737	3	13183
1757	7	N
1793	11	2143
1805	19	2011
1809	3	N
1817	23	471901
1835	367	19
1841	7	N
1917	71	2203
1927	41	3
1939	7	3
1963	151	3
1977	3	N
1981	7	3
2009	7	130261
2021	43	215077
2023	7	3
2033	19	N
2049	3	N
2073	3	N
2077	31	18211
2157	3	N
2173	53	3
2189	11	3313
2191	7	3
2201	31	N
2219	7	13
2241	3	N
2257	37	31
2261	7	4951
2313	3	N
2321	11	109987
2359	7	3
2369	23	431887
2413	19	8707
2419	41	3
2429	7	N
2443	7	3
2469	3	1063
2493	3	N

Next we eliminate the remaining cases of n, considering first those where N has but 2 non-trivial factors. We consider first all cases where neither factor of N is of the form $n_i^2 + n_i + 1$. By Ostrom's theorem 1, neither factor can be of type I, hence both must be of type II. By Ostrom's theorem 3, S divides $\Phi_{i=1,2}(N_i)$ where N_i is a factor of N, and S must be odd, also one of Ostrom's theorems 3.1 or 3.2 must hold. In each case we obtain a contradiction as to the order of S. We list the details below:

n	N $=N_1N_2$	$(n, \Phi N_1, \Phi N_2)$ or $(n+1, \Phi N_1, \Phi N_2)$	Contradiction
1883 = 7•269	3547573=199•17827	3	$7^3 \not\equiv$ (mod N)
1919 =19•101	3684481=79•46639	3	$19^3 \not\equiv$ (mod N)
1937 =13•149	3753907=1039•3613	3	$13^3 \not\equiv$ (mod N)
1967 = 7•281	3871057=223•17359	1	$7^2 \not\equiv$ (mod N)
2007 =32•223	4030057=109•36973	9	$3^9 \not\equiv$ (mod N)
2147 =19•113	4611757=547•8431	3	$19^6 \not\equiv$ (mod N)
2225 $=5^2$•89	4952851=109•45439	3	$5^6 \not\equiv$ (mod N)
2231 =23•97	4979593=193•25801	3	$23^{24} \not\equiv$ (mod N)

Now we consider the cases where N has but 2 non-trivial factors, exactly one factor N_1 which is of the form $n_i^2 + n_i + 1$, and a factor N_2 which is not of this form. For n = 1739 = 37•47, N = 157•19273 = 3025861 we find from a table of indices that the order of 37 (mod 157) is 39, and that $37^{39} \not\equiv 0 \pmod N$, hence 157 is a factor of type I. $157 = 12^2 + 12 + 1$, but there is no difference set for n =12, hence a contradiction to Ostrom's theorem 1. For n = 1651,

= 1865, 1959, 2353, 2427, a difference set exists modulo N_1. By theorem 1, N_2 must be a factor of type II hence Ostrom's theorem 3.3 can be applied. In each case it was verified that N_1 is a factor of type I. By Ostrom's theorem 3.3, S divides $n - n_1$ and by theorem 3, S is odd but in each case we find a contradiction to this, and hence no difference set is possible for those values of n. We list the details below. (Note: α is the order of the multiplier modulo N_1, $N = N_1 \cdot N_2$).

n	N_1	N_2	α	$n-n_1$	Contradiction
$1651=13\cdot127$	3	909151	$13\equiv1 \pmod 3$	1650	$13^{825}\not\equiv1 \pmod N$
$1865=5\cdot373$	31	112261	$5^3\equiv1 \pmod{31}$	1860	$5^{465}\not\equiv1 \pmod N$
$1959=3\cdot653$	13	295357	$3^3\equiv1 \pmod{13}$	1956	$3^{489}\not\equiv1 \pmod N$
$2353=13\cdot181$	3	1846321	$13\equiv1 \pmod 3$	2352	$13^{147}\not\equiv1 \pmod N$
$2427=3\cdot809$	13	453289	$3^3\equiv1 \pmod{13}$	2426	$3^{303}\not\equiv1 \pmod N$

We have remaining the case where $n = 2071 = 19\cdot109$, $N = 4291113 = 3\cdot31\cdot46141$. 31 and 3 are both prime factors of type I, and from our table of indices, 19 is of order 15 (mod 31). Also since $19 \equiv 1 \pmod 3$ we have $19^{15} \equiv 1 \pmod{3\cdot31}$. Now we apply Ostrom's theorem 1 letting $31 = q^t$ with $t = 19$ and $\alpha = 15$. Then $N_1 = (19^{15} - 1, N) = 3\cdot31$. But $3\cdot31 = 93$ which is not of the form $n_1^2 + n_1 + 1$, hence a contradiction to theorem 1, and no difference set can exist.

This eliminates all composite values of n less than 2501 as possible values for difference sets.

REFERENCES

[1] James Singer, A THEOREM IN FINITE PROJECTIVE GEOMETRY AND SOME APPLICATIONS TO NUMBER THEORY, Transactions of the American Mathematical Society, 43 (1938), 377-385.

[2] T. A. Evans and H. B. Mann, ON SIMPLE DIFFERENCE SETS, Sankhyā: The Indian Journal of Statistics, 11 (1951), 357-364.

[3] Marshall Hall, CYCLIC PROJECTIVE PLANES, Duke Mathematical Journal, 14 (1947), 1079-1090.

[4] T. G. Ostrom, CONCERNING DIFFERENCE SETS, Canadian Journal of Mathematics, 5 (1953), 421-424.

[5] H. B. Mann, SOME THEOREMS ON DIFFERENCE SETS, Canadian Journal of Mathematics, 4 (1952), 222-226.